King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Department of Computer Engineering

COE 451 – Computer and Network Security (T142)

Homework # 06 ***(due date & time: Thursday 16/04/2015 during class period)***

Problem # 1: On a particular system, all passwords are 8 characters, there are 128 choices for each character, and there is a password file containing the hashes of 2^{12} passwords. Trudy has a dictionary of 2^{24} passwords, and the probability that a randomly selected password is in her dictionary is 1/4. Work is measured in terms of the number of hashes computed.

a. Suppose that Trudy wants to recover Alice's password. Using her dictionary, what is the expected work for Trudy to crack Alice's password, assuming the passwords are not salted?
b. Repeat part a, assuming the passwords are salted.
c. What is the probability that at least one of the passwords in the password file appears in Trudy's dictionary?

Problem # 2: Suppose all passwords on a given system are 8 characters and that each character can be any one of 128 different values. The passwords are hashed (with a salt) and stored in a password file. Now suppose Trudy has a password cracking program that can test 128 passwords per second. Trudy also has a dictionary of 2^{24} common passwords and the probability that any given password is in her dictionary is 1/4. The password file on this system contains 512 password hashes.

a. How many different passwords are possible?
b. How long, on average, will it take Trudy to crack the administrator's password?
c. What is the probability that at least one of the 512 passwords in the password file is in the dictionary?
d. What is the expected work for Trudy to recover any one of the passwords in the password file?

Problem # 3: Solve problem 20 of Chapter 7 of the textbook.

Problem # 4: Suppose that when a fingerprint is compared with one other (nonmatching) fingerprint, the chance of a false match is 1 in 10^{10}, which is approximately the error rate when 16 points are required to determine a match as in the British legal standard. Suppose that the FBI fingerprint database contains 10^8 fingerprints.

a. How many false matches will occur when 1,000,000 suspect fingerprints are each compared with the entire database?
b. For any individual suspect, what is the chance of a false match?

Problem # 5: Suppose that a particular iris scan systems generates 64-bit iris codes instead of the standard 2048-bit iris codes mentioned in chapter 7. During the enrollment phase, the following iris codes (in hex) are determined.

User	Iris code
Alice	DE439AD598EF5147
Bob	AC8B7A1425369584
Charlie	886611335599CCBB

During the recognition phase, the following iris codes are obtained.

User	Iris code
U	C8A96E16273E9104
V	984641B315D1C4B9
W	56258BE6CD769DFC
X	24ED6B2770AF593F
Y	564B9A159A6F5D41

Use the iris codes above to answer the following questions.

a. Use the formula in equation (7.1) to compute the following distances: *d*(Alice, Bob), *d*(Alice, Charlie), *d*(Bob, Charlie).
b. Assuming that the same statistics apply to these iris codes as the iris codes discussed in Section 7.4.2.3, which of the users, U,V,W,X,Y, is most likely Alice? Bob? Charlie? None of the above?